U.S. Department of Justice

United States Attorney
Eastern District of New York

DSS:CMP
F. #2011R00414

271 Cadman Plaza East
Brooklyn, New York 11201

June 21, 2013

By ECF

The Honorable John Gleeson
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Imran Elahi, Criminal Docket No. 12-246 (JG)

Dear Judge Gleeson:

In anticipation of the defendant Imran Elahi's sentencing on June 28, 2013, the government respectfully submits this letter to address the defendant's offense conduct, the procedural history of the case and the appropriate Guidelines calculation. The government intends to address additional factors for the Court's consideration at sentencing in two separate submissions.

I. The Offense Conduct

As described in paragraph 4 of the Presentence Investigation Report ("PSR"), dated November 15, 2012, the United States Secret Service ("Secret Service") has been investigating an international conspiracy to hack into the computer systems of financial institutions and other businesses in the United States and elsewhere for the purpose of stealing confidential financial account information (including personal identification numbers ("PINs")), which the hackers in turn sell to individuals in the United States and other countries over the Internet. The conspirators generally transmit this information through an array of online communication mechanisms, such as instant messaging and email. The purchasers of the stolen financial information use the account numbers to encode plastic cards, such as gift cards, which they then use to withdraw currency from automated teller machines ("ATMs") located at banks

in the United States and elsewhere in a scheme known as a "PIN cashout" or "PIN cashing." The use of unauthorized credit and debit cards is generally known as "carding." The participants in such activities who are responsible for making the fraudulent withdrawals, known as "cashers," ultimately share a portion of their illicit proceeds with the organizers of the cashouts, transmitting the funds using wire transfers and various forms of electronic currency, such as Liberty Reserve.

In certain PIN cashout operations, the conspirators target credit card processors that process transactions for Visa and MasterCard prepaid debit cards. As a result of extensive network intrusions, the hackers increase the withdrawal limits on such prepaid debit cards in a scheme known in the PIN cashout and carding community as an "unlimited operation." In such operations, hackers in the past have successfully manipulated account balances and in some cases security protocols to effectively eliminate any withdrawal limits on individual accounts. As a result, even a few compromised bank account numbers can result in tremendous financial loss to the victim financial institution. Successful unlimited operations require a high degree of technical proficiency, coordination and patience on the part of the criminal actors.

Using a variety of investigative means described in the PSR, included court-authorized search warrants of email accounts used by the defendant and his coconspirators, the government determined that the defendant participated in an unlimited operation in February 2011 that targeted Fidelity Information Services ("FIS"), a publicly traded credit card processing company based in the United States. PSR ¶¶ 6-8. Specifically, the coconspirators responsible for the intrusion targeted several prepaid debit card accounts serviced by FIS that had been issued by the American Red Cross to provide disaster relief to victims. PSR ¶ 8. This operation resulted in over $13 million in financial loss worldwide in less than two days. Id. The defendant was personally responsible for using and disseminating one compromised FIS prepaid debit card, which he received from certain leaders of the conspiracy and disseminated to coconspirators in Mexico and elsewhere, resulting in approximately $1.44 million in fraudulent withdrawals. Id.

After his arrest, the government learned that the defendant had become involved in carding activities in 2003 or 2004, and participated in carding forums and other forms of online communications where stolen account information, such as compromised credit and debit cards, are bought and sold. In 2008, the defendant participated in a major cashout operation that targeted debit cards issued by RBS WorldPay, a credit card processor based in Atlanta, Georgia. The RBS WorldPay operation resulted in over $9 million in financial loss to the victim institution and several members of that scheme have been prosecuted in the Northern District of Georgia.[1] As in the FIS unlimited operation, the defendant's role in the RBS WorldPay operation was to disseminate the compromised account information to managers of cashers in

[1] See United States v. Viktor Pleshchuk, et al., 09 CR 491 (N.D.Ga.).

various countries around the world. Those managers paid a portion of the proceeds they received to the defendant, who in turn paid a portion to the organizers of the operation. The defendant himself earned approximately $250,000 to $300,000 from his criminal activities during the charged time period (2005 to 2012).

II. Arrest and Guilty Plea

Dutch authorities arrested the defendant in the Netherlands on March 8, 2012, pursuant to a provisional arrest request made by this Office. PSR ¶ 12. He waived extradition and arrived in the Eastern District of New York on April 10, 2012. Id. Shortly thereafter, on May 11, 2012, the defendant pleaded guilty to a two-count information charging access device fraud conspiracy from January 2005 to March 2012 and substantive access device fraud during the same time period. As part of his plea agreement, the defendant agreed to forfeit $50,000 in criminal proceeds to the government; he paid $25,000 toward the forfeiture judgment at the time of his plea and is expected to pay the remainder when he is sentenced. The defendant also stipulated to a loss amount of over $20 million for purposes of calculating his advisory Guidelines range based on the financial loss that was either directly attributable or reasonably foreseeable to him as a result of his participation in the RBS and FIS operations, which resulted in approximately $9 million and $14 million in loss, respectively, as well as the significant number of compromised access device card numbers (well over 10,000) that he possessed or sold. Approximately 354 financial institutions, including the issuing institutions for the compromised access device card numbers, were victims of the defendant's criminal cashout and carding activities since 2005. See Addendum to the PSR dated May 10, 2013, page 1.

III. Guidelines Calculation

The government agrees with the Probation Department's calculation of a total offense level of 35, based on an adjusted offense level of 38 and a three-point reduction for acceptance of responsibility. PSR ¶¶ 17-33. At Criminal History Category I, the defendant's advisory Guidelines range of imprisonment is 168 to 210 months. PSR ¶ 66.

Respectfully submitted,

LORETTA E. LYNCH
United States Attorney

By: /s/ Cristina M. Posa
Cristina M. Posa
Assistant U.S. Attorney
(718) 254-6668

cc: Johanna Zapp, Esq. (via ECF)